D33.6

Legal analysis of eSignature services

Document Identification	
Date	30/07/2015
Status	Final
Version	1.0

Related SP / WP	SP3/WP33	**Document Reference**	D33.6
Related Deliverable(s)	D22.6, D33.1-D33.5	**Dissemination Level**	PU
Lead Participant	KUL	**Lead Author**	Jessica Schroers (KUL)
Contributors	Jessica Schroers (KUL) Brendan van Alsenoy (KUL) Colette Cuijpers (RU)	**Reviewers**	Hannah Obersteller (ULD) Christof Rath (TUG)

Abstract: This deliverable provides a comprehensive analysis of the legal framework surrounding the provision of FutureID eSignature services. It does this by first showing the bigger picture regarding electronic signatures, the situation before the eIDAS Regulation and providing an overview of the Belgian and German provisions on electronic signatures. The second part focuses on the new eIDAS Regulation. It compares the provisions regarding electronic signatures of the Regulation with the provisions of the eSignature Directive. By doing this it provides an overview of the requirements for electronic signatures, in particular qualified electronic signatures. Finally the third part analyses the application to the FutureID eSign service, in a question-answer format.

This document is issued within the frame and for the purpose of the *FutureID* project. This project has received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under Grant Agreement no. 318424.

1. Executive Summary

This deliverable provides a comprehensive analysis of the legal framework surrounding the provisioning of FutureID eSignature Services. In doing so, it first provides an overview of the subject of electronic signatures, delineating the difference between digital and electronic signatures. Electronic signatures are a legal concept, established European wide by the eSignature Directive and influenced by the technology of digital signatures, but at the same time formulated intentionally technologically neutral. The eSignature Directive ensured a certain harmonization with regard to the national law, which needed to implement the provisions of the Directive. This deliverable includes a short overview of German and Belgian signature law. However, the main focus is on the new eIDAS Regulation. The Regulation entered into force on the 17th of September 2014 and the provisions for trust services will apply from the 1st of July 2016, while the eSignature Directive will be repealed from that day. As a Regulation, the provisions of the eIDAS Regulation are directly applicable and do not need to be implemented in national law.

In order to provide an overview of the legal requirements for electronic signatures, the provisions of the eIDAS Regulation regarding electronic signatures were compared with the provisions of the eSignature Directive, and an overview of the most important requirements was given. The difference between advanced and qualified electronic signatures is important. Advanced electronic signatures are electronic signatures which are uniquely linked to the signatory, capable of identifying the signatory, created with a private key that the signatory can, with a high level of confidence, use under his sole control, and are linked to the signed data in such a way that any change in the data is detectable. This already provides a certain reliability regarding the legal effect of the signature, however, in order to be considered equal to a handwritten signature, the electronic signature needs to be qualified. Qualified electronic signatures are based on advanced electronic signatures, yet have stricter and more extensive requirements.

The focus of the FutureID eSign service is on advanced electronic signatures. However, the analysis also assesses the requirements to use the eSign service for qualified electronic signatures. It is in principle possible to use the FutureID eSign service with qualified electronic signatures, since the eSign service provides a generic interface for electronic signatures, which can be used with different certificates and electronic signature creation devices. Therefore, by using the required qualified certificate for electronic signatures and generating the signature with a qualified electronic signature creation device, it is also possible to create qualified electronic signatures. These qualified electronic signatures then can be verified by using a qualified electronic signature verification service.

It could be established that the eSign service will not fall under the provisions for TSPs of the eIDAS Regulation as it does not constitute a trust service. In addition it has been assessed whether the main formats supported by the eSign service, PAdES, XAdES and CAdES, can still

be considered advanced electronic signatures under the eIDAS Regulation and whether signing with the eSign service using remote (qualified) electronic signature solutions will result in a legally relevant signature.

2. Document Information

2.1 Contributors

Name	Partner
Jessica Schroers	KUL
Brendan van Alsenoy	KUL
Colette Cuijpers	RU

2.2 History

Version	Date	Author	Changes
0.1	04.09.2014	Jessica Schroers	Initial draft
0.9	27.07.2015	Jessica Schroers, Brendan van Alsenoy, Colette Cuijpers	Final draft
1.0	22.09.2015		Final version

2.3 Table of Figures

2.4 Table of Acronyms

BGB Bürgerliches Gesetz Buch

BW Burgerlijk Wetboek

CSP Certification Service Provider

EU European Union

HSM Hardware Security Modul

OJ Official Journal

PKI Public Key Infrastructure

QESCD Qualified Electronic Signature Creation Device

QTSP Qualified Trust Service Provider

SigG Signaturgesetz

SigV Signaturverordnung

SSCD Secure Signature Creation Device

TSP Trust Service Provider

ZPO Zivilprozessordnung

2.5 Referenced Documents

S. Baker and M. Yeo, 'Survey of international electronic and digital signature initiatives, Steptoe & Johnson LLP', Internet Law and Policy Forum.

A. Barofsky, 'The European Commission's Directive on electronic signatures: Technological "Favoritism" towards digital signatures', 24 B.C. Int'l & Comp. L. Rev. 145, 2000.

J. Dumortier, S. Kelm, et.al., 'The legal and market aspects of electronic signatures – Legal and market aspects of the application of Directive 1999/93/EC and practical applications of electronic signatures in the Member States, the EAA, the Candidate and the Accession Countries', Study for the European Comission within the eEurope 2005 framework, 2003.

J. Dumortier, *ICT Recht*, Acco, Leuven, 2013.

P. van Eecke, *De handtekening in het recht – van pennentrek tot elektronische handtekening*, Larcier, Gent, 2004.

P. Van Eecke & M. Truyens , 'Benchmarking of existing national legal e-business practices'. DG ENTR/04/68. Country report – Belgium, 14 June 2006.

European Commission, 'Feasibility study on an electronic identification, authentication and signature policy (IAS)', Final Report, Luxembourg, Publications Office of the European Union, 2013.

ETSI TS 101 903: XML Advanced Electronic Signatures (XAdES).

ETSI TS 102 778-3: PDF Advanced Electronic Signature Profiles (PAdES).

ETSI TS 101 733: CMS Advanced Electronic Signatures (CAdES).

R.L. Rivest, A. Shamir, L. Adleman, 'A method for obtaining digital signatures and public-key cryptosystems', Communications of the ACM, Volume 21 Issue 2, ACM New York, Feb. 1978, 120-126.

A. Roßnagel, 'Der Anwendungsbereich der eIDAS-Verordnung – Welche Regelungen des deutschen Rechts sind weiterhin für elektronische Signaturen anwendbar?', MMR, 2015, 359-364.

A.Roßnagel, 'Neue Regeln für sichere elektronische Transaktionen: Die EU-Verordnung über elektronische Identifizierung und Vertrauensdienste', NJW 2014, 3686-3692.

A. Roßnagel, 'Fremderzeugung von qualifizierten Signaturen? - ein neues Geschäftsmodell und seine Rechtsfolgen', MMR, 2008, 22-28.

C. Seegebarth, 'Perspektiven aus der eIDAS-Verordnung', DuD, 10, 2014, 675-678.

S. Sieber, T. Nöding, 'Die Reform der elektronischen Unterschrift', ZUM 2001, 199 -210.

SMART 2012/0001, Phase II - Electronic signatures in public services, Version 2.1, 5 June 2014.

Legislation

European:

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L281, 23.11.95 (Data Protection Directive)

Explanatory Memorandum COM(98)297, Proposal for a European Parliament and Council Directive on a common framework for electronic signatures (98/C 325/04) (Text with EEA relevance) COM(1998) 297 i final - 98/0191(COD).

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, Official Journal of the European Union, L13/12, 19.1.2000 (eSignature Directive).

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Official Journal of the European Union, L 257/73, 28.8.2014, (eIDAS Regulation).

German:

SigG1997: Gesetz zur digitalen Signatur (Introduced as art. 3 of the ‚Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste' from 22.7.1997, BGBl I nr. 52, 1870).

Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste' from 22.7.1997, BGBl I nr. 52, 1870.

BT 14/4987, Gesetzentwurf der Bundesregierung, „Entwurf eines Gesetzes zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr“, 14.12.2000.

SigG: Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876), das zuletzt durch Artikel 4 Absatz 111 des Gesetzes vom 7. August 2013 (BGBl. I S. 3154) geändert worden ist.

Gesetz über die Verwendung elektronischer Kommunikationsformen in der Justiz (Justizkommunikationsgesetz – JkomG), BGBl I Nr. 18, 29.3.2005.

Zivilprozessordnung in der Fassung der Bekanntmachung vom 5. Dezember 2005 (BGBl. I S. 3202; 2006 I S. 431; 2007 I S. 1781), die zuletzt durch Artikel 1 des Gesetzes vom 8. Juli 2014 (BGBl. I S. 890) geändert worden ist.

Belgian:

Wet van 9 juli 2001 houdende vaststelling van bepaalde regels i.v.m. het juridische kader voor elektronische handtekeningen en certificatiediensten, BS 29 september 2001.

Wet van 20 oktober 2000 tot invoering van het gebruik van telecommunicatiemiddelen en van de elektronische handtekening in de gerechtelijke en de buitengerechtelijke procedure, BS 22 december 2000.

3. Table of Contents

4. Project Description

The *FutureID* project builds a comprehensive, flexible, privacy-aware and ubiquitously usable identity management infrastructure for Europe, which integrates existing eID technology and trust infrastructures, emerging federated identity management services and modern credential technologies to provide a user-centric system for the trustworthy and accountable management of identity claims.

The *FutureID* infrastructure will provide great benefits to all stakeholders involved in the eID value chain. Users will benefit from the availability of a ubiquitously usable open source eID client that is capable of running on arbitrary desktop PCs, tablets and modern smart phones. *FutureID* will allow application and service providers to easily integrate their existing services with the *FutureID* infrastructure, providing them with the benefits from the strong security offered by eIDs without requiring them to make substantial investments.

This will enable service providers to offer this technology to users as an alternative to username/password based systems, providing them with a choice for a more trustworthy, usable and innovative technology. For existing and emerging trust service providers and card issuers *FutureID* will provide an integrative framework, which eases using their authentication and signature related products across Europe and beyond.

To demonstrate the applicability of the developed technologies and the feasibility of the overall approach *FutureID* will develop two pilot applications and is open for additional application services who want to use the innovative *FutureID* technology.

Future ID is a three-year duration project funded by the European Commission Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 318424.

5. Outline and scope

This deliverable provides a comprehensive analysis of the legal framework surrounding the provisioning of FutureID eSignature services. Particular attention is on the new eIDAS Regulation and its provisions on electronic signatures. The deliverable is divided into three parts. The first part shows the bigger picture regarding electronic signatures. Here, it is explained what exactly electronic signatures are, how the different forms relate to each other and how they are accepted in court. Since the eSignature Directive required national implementation, this part of the deliverable depicts the Belgian and German provisions on electronic signatures as an example. The second part focuses on the new eIDAS Regulation. It compares the provisions regarding electronic signatures of the Regulation with the provisions of the eSignature Directive. By doing this it provides an overview of the requirements for electronic signatures, in particular qualified electronic signatures. Finally, the third part analyses the application to the FutureID eSign service, in a Q&A format.

6. What are electronic signatures?

Signatures fulfil an essential role in the legal order.[1] The act of signing a document can fulfil various functions, ranging from closing the document to identifying the signatory and expressing the intention of the signatory. [2]

With the increase of e-commerce, many documents turned electronic, and in the course of this it became necessary to find a way to electronically sign the documents. In order to sign electronically especially the digital signature technology is used in practice.

Before proceeding with this section, it is necessary to clarify the difference between 'electronic signature' and 'digital signature'. Even though they are often used interchangeably, these are two different concepts. 'Digital signature' is a technological concept, based on an encryption technology and used to provide integrity and non-repudiation[3] of a message.[4] 'Electronic signature' on the other hand is a legal concept, which is independent of the used technology and refers to the signature of electronic documents. A digital signature can be used to sign electronically. However, the digital signature technology can also be used for other purposes than electronic signatures. Therefore, not every digital signature is also an electronic signature. Likewise the electronic signature as a broad, technology neutral, concept includes different ways of signing, and not every electronic signature is made with digital signature technology.

[1] P. van Eecke, "De handtekening in het recht – van pennentrek tot elektronische handtekening", Larcier, Gent, 2004, p.268.

[2] In Germany seven functions are described: Closure function, perpetuation function, identity function, further the signature proves that the information on the document is from the signatory (authenticity function), that the signature is genuine (verification function), it provides evidence (evidence function) and through the conscious act of signing the signatory will be alerted of the legally binding function of the signature (warning function). It has been stressed that an electronic signature needs to be able to fulfil all these requirements in order to be equivalent to a handwritten signature (see BT 14/4987, Gesetzentwurf der Bundesregierung, „Entwurf eines Gesetzes zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr", 14.12.2000). In Belgium a signature is in general considered to have two functions (identification and the expression of the intention of the signatory), see P. van Eecke, "De handtekening in het recht – van pennentrek tot elektronische handtekening", Larcier, Gent, 2004, p. 191. Patrick van Eecke identifies in his book two additional functions: the security function and the ritual/ceremonial function.

[3] The ability to link an action to an identity in such a way that the person cannot claim they did not perform the action at a later date.

[4] See R.L.Rivest, A. Shamir, L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, Volume 21 Issue 2, ACM New York, Feb. 1978, p. 120-126.

With regard to electronic contracts, the problem arose that the legal effect of electronically signed contracts was not certain.[5] Therefore, different countries started to implement national legislation with regard to the validity of electronic/digital signatures.[6]

The development of divergent legislations on electronic signatures could potentially inhibit the use of electronic signatures in the internal market. The problem was that for conflicting legal and technical requirements under different jurisdictions, cross-border use of electronic signatures was difficult or even impossible.[7] The European Commission, therefore, drafted a Directive, the eSignature Directive 1999/93/EC, which attempted to harmonize the legal framework for the use of electronic signatures and establish a set of criteria, which form the basis for legal recognition of electronic signatures.[8]

The Directive introduced three different types of electronic signatures: 'electronic signatures', 'advanced electronic signatures' and 'qualified electronic signatures'[9]. Particular requirements apply to the different types of signatures, and also the legal effects are not the same.

The term 'electronic signature' in the Directive has a very broad definition, which is deliberately technology neutral. It defines an 'electronic signature' as "data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication".[10] Therefore, for example, writing a name under an e-mail is considered an electronic signature. However, this is not as secure as a handwritten signature, since anybody can write any name under an e-mail, without even having to forge the handwriting.

Advanced electronic signatures provide a higher level of confidence than 'ordinary' electronic signatures. Electronic signatures are considered advanced if they are uniquely linked to the signatory; capable of identifying the signatory; created using means that the signatory can

[5] A. Barofsky, "The European Commission's Directive on electronic signatures: Technological "Favoritism" towards digital signatures", 24 B.C. Int'l & Comp. L. Rev. 145, 2000, p. 1.

[6] Germany introduced in 1997 a first electronic signature legislation 'Gesetz zur digitalen Signatur' (SigG1997) (Introduced as art. 3 of the 'Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste' from 22.7.1997, BGBl I nr. 52, 1870) to create a framework in which digital signatures can be considered secure and falsification of signatures or signed data can be reliably recognized. For signatures that fulfilled the requirements of the SigG1997, the law considered as (only) legal consequence an authenticity assumption. It did not equate the digital signature with a normal signature. See S.Sieber, T.Nöding, Die Reform der elektronischen Unterschrift, ZUM 2001, 199, p. 200.

[7] Stewart Baker and Matthew Yeo, Survey of international electronic and digital signature initiatives, Steptoe & Johnson LLP, Internet Law and Policy Forum, available at http://www.ilpf.org/groups/survey.htm#IVA.

[8] Explanatory Memorandum COM(98)297, p. 6.

[9] Qualified electronic signatures were not termed as such, but as "advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device". However, the literature generally used the term 'qualified electronic signature', which was also used in the national implementation of the Directive in certain countries (e.g. Germany). The term has now been taken up in the eIDAS Regulation.

[10] Art.2 (1) Directive 1999/93/EC.

maintain under his or her sole control, and are linked to the data to which they relate in such a manner that any subsequent change of the data is detectable.[11] The requirements for an advanced electronic signature are phrased technology neutral. However, the technological solution that can fulfil them at this point of time, and which was in the back of the mind of the Commission when drafting the Directive, is the digital signature. Here, it is important to note that digital signature technology can be used for entity authentication as well as for the creation of electronic signatures (an example is an electronic identity card with two key pairs, one for access control (entity authentication) and one for electronic signatures (data authentication)).[12] Only the use for electronic signatures falls under the Directive.

A qualified electronic signature must fulfil even more requirements in order to be considered qualified, and is therefore deemed more secure. Qualified electronic signatures are advanced electronic signatures which are additionally based on a qualified certificate provided by a certification service provider who fulfils the requirements laid down in Annex II of the Directive[13], and are created using a secure signature-creation device (SSCD). In view of this increased security the qualified electronic signature is considered equivalent to a handwritten signature. Art. 5 of the eSignature Directive states that 'qualified' electronic signatures satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data. It should be ensured that electronic signatures can be used as evidence in legal proceedings in all Member States.[14] Simple 'electronic signatures' are not considered equivalent, but, according to art. 5 (2), just because they are not 'qualified' or in electronic form does not mean that they can be denied legal effect and admissibility as evidence in legal proceedings (non-discrimination rule).

6.1 National electronic signature legislation examples

This section provides an overview of the electronic signature legislation of Germany and Belgium. These two countries are chosen as example, as Germany was among the first countries to introduce electronic signature legislation, even before the eSignature Directive was introduced. On the other hand, Belgium introduced electronic signature legislation only after the introduction of the Directive, and stayed in their implementation closely to the eSignature Directive.

[11] Art. 2 (2) Directive 1999/93/EC.
[12] Dumortier, J., Kelm, S., a.o., "The legal and market aspects of electronic signatures – Legal and market aspects of the application of Directive 1999/93/EC and practical applications of electronic signatures in the Member States, the EAA, the Candidate and the Accession Countries", Study for the European Commission within the eEurope 2005 framework, 2003, p. 30.
[13] Art. 2 (10) Directive 1999/93/EC.
[14] Recital 21 Directive 1999/93/EC.

6.1.1 Electronic signatures in Germany:

Germany started early in 1997 with their own electronic signature legislation 'Law for the digital signature'('Gesetz zur digitalen Signatur' (SigG1997)[15]). The goal was to create a framework in which digital signatures can be considered secure and falsification of signatures or signed data can be reliably recognized.[16] For this, it aimed to build a privately organised infrastructure under public supervision.[17] Only for signatures which fulfilled the requirements of the SigG1997, the law considered as (only) legal consequence an authenticity assumption.[18] It did not equate the digital signature with a handwritten signature.[19] Only accredited CSPs could issue signatures that are conform to the signature law.[20] The law specified in §15 SigG1997 that digital signatures which can be verified at the hand of a public signature key connected to a foreign certificate from another Member State or EEC (European Economic Community) country[21], can be considered equal to digital signatures according to the SigG1997, if they provide the same level of security.

After the introduction of the eSignature Directive, Germany had to change their law, since some provisions of the 1997 law, especially regarding the security level and the accreditation obligation, were not conform to the European Directive. Especially the German accreditation obligation was not conform to the Directive, since the Directive considered obligatory accreditation as a barrier to the free movement of goods and services in the internal market.[22] Therefore, Germany introduced a new signature law (also named 'Signaturgesetz' (SigG))[23] in 2001, which was conform to the Directive, and kept the possibility of an accreditation in the form of a voluntary accreditation, as was possible under the Directive.[24]

---

[15] Introduced as art. 3 of the 'Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste' from 22.7.1997, BGBl I nr. 52, 1870.
[16] §2 (1) SigG1997.
[17] S.Sieber, T.Nöding, Die Reform der elektronischen Unterschrift, ZUM 2001, 199, p. 200.
[18] Idem.
[19] P. Van Eecke, De Handtekening in het recht, Larcier Gent, 2004, p. 368.
[20] S.Sieber, T.Nöding, Die Reform der elektronischen Unterschrift, ZUM 2001, 199, p. 200.
[21] Or a third country if appropriate agreements exist (§ 15 (2) SigG1997).
[22] Recital 4 Directive 1999/93/EC.
[23] Current version: Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876), das zuletzt durch Artikel 4 Absatz 111 des Gesetzes vom 7. August 2013 (BGBl. I S. 3154) geändert worden ist.
[24] That the possibility of voluntary accreditation was introduced in the Directive was a result of Germany's intervention in order to keep the investments of their two biggest accredited certification providers, see S.Sieber, T.Nöding, Die Reform der elektronischen Unterschrift, ZUM 2001, 199, p. 202. The new law further included provisions concerning fines for administrative offenses, which was not expressly stipulated in the Directive, and was seen critical as potential discrimination of German CSPs in S.Sieber, T.Nöding, Die Reform der elektronischen Unterschrift, ZUM 2001, 199, p. 203. §21 SigG details the fines which can be up to a maximum of 10.000 or 50.000 Euro for specific administrative offenses and was introduced, arguing that it is a part of the, by art. 3 (3) Directive 1999/93/EC required, supervision system.

Besides the introduction of the SigG, also another law was introduced in 2001, the 'Law for adjustment of the formal requirements to modern legal transactions' ('Gesetz zur Anpassung der Formvorschriften an den modernen Rechtsgeschäftsverkehr'[25], which amended several laws that had only accepted 'written form' before.[26] 'Written form' ("Schriftform") is the requirement that certain documents are only accepted if they are in writing and personally signed. Instead of changing every single law that required written form, some laws were amended, as for instance general provision on form requirements in the civil law. In § 126 of the German Civil Code (BGB) another paragraph got introduced stating that the written form can be exchanged by the electronic form, as long as the law does not provide differently.[27] Additionally, § 126a BGB and § 126b BGB were included, which specify electronic form and text form. For the electronic form it is important that the issuer of the declaration must add his name and sign with a qualified electronic signature, in order to replace the written form if it is prescribed by statute.[28] In case of a contract, each of the parties must provide their counterpart(s) with a qualified electronic signature.[29]

Article 5 (1) of the eSignature Directive required that electronic signatures in principle can be used as evidence in legal proceedings. In Germany this has always been possible, since electronic documents including their electronic signatures can be used as "Augenscheinbeweis" (evidence by judicial inspection), which means that the judge examines the document and then decides whether it is authentic.[30] In § 371 ZPO[31] it is now included that "if an electronic document is object of the proof, the evidence can be formed by presentation or transmission of the data file. § 371a ZPO[32] even specifically prescribes the evidence value of electronic documents, and states that for private electronic documents which are signed with a qualified electronic signature, the rules over the evidence value of private documents ('Urkunde') can be applied mutatis mutandis. The appearance of authenticity can only be unsettled with facts which justify strong doubts that the statement has been provided by the signature key owner.

[25] BT 14/4987, Gesetzentwurf der Bundesregierung, 'Entwurf eines Gesetzes zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr', 14.12.2000.
[26] S.Sieber, T.Nöding, Die Reform der elektronischen Unterschrift, ZUM 2001, 199, p. 206.
[27] § 126 (3) BGB.
[28] § 126a (1) BGB.
[29] § 126a (2) BGB
[30] S.Sieber, T.Nöding, Die Reform der elektronischen Unterschrift, ZUM 2001, 199, p. 206.
[31] German Code of Civil Procedure: Zivilprozessordnung in der Fassung der Bekanntmachung vom 5. Dezember 2005 (BGBl. I S. 3202; 2006 I S. 431; 2007 I S. 1781), die zuletzt durch Artikel 1 des Gesetzes vom 8. Juli 2014 (BGBl. I S. 890) geändert worden ist.
[32] Introduced later in 2005 by the 'Gesetz über die Verwendung elektronischer Kommunikationsformen in der Justiz (Justizkommunikationsgesetz – JkomG)', BGBl I Nr. 18, 29.3.2005.

6.1.2 Electronic signatures in Belgium

In Belgium the law historically did not include a definition of "signature", it was only defined in legal doctrine and case law.[33] From analysis of case law it could be concluded that a valid signature in Belgium is 'a with the hand personally placed written sign that refers to the identity of the signatory'.[34] This definition excluded the use of electronic signatures. The first legal definition of signatures, which then only related to electronic signatures, got introduced in 2000 with the 'Act of 20 October 2000 introducing the use of telecommunication tools and the electronic signature in the judicial and extra-judicial procedure' ('Wet van 20 oktober 2000 tot invoering van het gebruik van telecommunicatiemiddelen en van de elektronische handtekening in de gerechtelijke en de buitengerechtelijke procedure, BS 22 december 2000'). Here Belgium introduced the possibility to use electronic signatures in the Belgian Civil Code, to be more exact in art. 1322 section 2: "*Kan, voor de toepassing van dit artikel, voldoen aan de vereiste van een handtekening, een geheel van elektronische gegevens dat aan een bepaalde persoon kan worden toegekend en het behoud van de integriteit van de inhoud van de akte aantoont.*" ('Can, for the application of this article, satisfy the requirements of a signature, a unity of electronic data which can be linked to a specific person and proves the integrity of the document.'). After the introduction of this provision, a judge in Belgium could not refuse an electronic signature only because it was in electronic form.

Even though art. 1322 section 2 of the Belgian Civil Code might have been sufficient,[35] Belgium later also implemented the eSignature Directive with a specific law "Wet van 9 juli 2001 houdende vaststelling van bepaalde regels i.v.m. het juridische kader voor elektronische handtekeningen en certificatiediensten",[36] which formed a very stringent implementation of the Directive.[37] However, a difference between the eSignature Directive and the Belgian implementation is for example that the Belgian law states in art. 4, §4, that a qualified electronic signature will be assimilated with a hand-written signature "irrespective of the fact that the signature has been made by a legal or a natural person".[38]

Belgian law defines two requirements for an electronic signature: that the signature can be linked to a specific person, and that the integrity of the document can be proven (authenticity of

[33] J. Dumortier, *ICT-recht*, Acco, Leuven, 2013, p. 123.
[34] P. Van Eecke, De Handtekening in het recht, Larcier Gent, 2004, p. 450.
[35] See opinion J. Dumortier, *ICT-recht*, Acco, Leuven, 2013, p. 128.
[36] Wet van 9 juli 2001 houdende vaststelling van bepaalde regels i.v.m. het juridische kader voor elektronische handtekeningen en certificatiediensten, BS 29 september 2001.
[37] Patrick Van Eecke & Maarten Truyens , Benchmarking of existing national legal e-business practices. DG ENTR/04/68. Country report – Belgium, 14 June 2006, http://ec.europa.eu/enterprise/sectors/ict/files/belgium_en.pdf, p.2.
[38] Idem.

the information).[39] However, the fulfillment of these two requirements does not automatically result in a valid signature. Validity can depend on further factors. For example it should result from the context, whether the electronic data fulfilling the two requirements is intended to be a signature.[40] Therefore, the judge has a certain margin to decide whether or not it is a valid signature.

Summarizing it can be said that in Belgium (1) No electronic signature can be denied legal effectiveness and admissibility as evidence in legal proceedings (art. 4, §5), (2) Electronic signatures can be used as an alternative for a handwritten signature for evidential purposes, as long as one can prove that the electronic signature forms a transformation of data from which with certainty the identity of the author and the integrity of the signed content follows (art. 1322 Civil Code), and (3) the qualified electronic signature automatically will be given the same legal value as a handwritten signature (art. 4, §4).[41]

[39] J. Dumortier, *ICT-recht*, p. 126.
[40] J. Dumortier, *ICT-recht*, p. 127.
[41] Patrick Van Eecke & Maarten Truyens , Benchmarking of existing national legal e-business practices. DG ENTR/04/68. Country report – Belgium, 14 June 2006, http://ec.europa.eu/enterprise/sectors/ict/files/belgium_en.pdf, p.2.

7. Requirements for electronic signatures in the eIDAS Regulation

This section provides an overview of the relevant provisions for an electronic signature. We will focus on the relevant provisions of the eIDAS Regulation and a comparison with the provisions of the eSignature Directive.

7.1 Electronic signatures according to eIDAS Regulation

The European Commission proposed on the 4th of June 2012 a Regulation on **e**lectronic **ID**entification and **A**uthentication **S**ervices (eIDAS). It was officially published in the OJ on 28 of August 2014[42] and entered into force on the 17th of September 2014. However, the Regulation will only apply starting from the 1st of July 2016, provided for some exceptions.[43] The eSignature Directive will be repealed with effect from the same date. The rules on trust services shall apply starting from the 1st of July 2016.[44]

While the eSignature Directive focused solely on electronic signatures, the eIDAS Regulation has a broader approach. One part concerns provisions regarding electronic identification, and another part concerns trust services. The part on trust services of the eIDAS Regulation does not only cover electronic signatures, but also other trust services such as electronic seals and time stamps. Even though the provisions of the eIDAS Regulation regarding electronic signatures are largely similar to the ones of the Directive, more specific definitions are used due to the broader focus. Since the Regulation also includes stipulations regarding electronic identity, the notion of identity is used with greater precision within the Regulation. We will provide here a short overview of the changes of the eIDAS Regulation in comparison to the eSignature Directive.

[42] Official Journal of the European Union, L 257/73, 28.8.2014, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:JOL_2014_257_R_0002&from=EN

[43] Immediately from entering into force the articles referring to implementation acts apply. The provisions relating to the notification of national eID schemes shall apply from the date of application of the implementing acts setting out minimum technical specifications, standards and procedures regarding the assurance levels, and regarding an interoperability framework. The date of application of the implementing acts is supposed to be 18 September 2015. Three years after this date, so supposedly 18 September 2018, article 6 on mutual recognition shall apply, however, Member States can decide to recognise notified identification schemes voluntarily already before that date.

[44] Art. 52 Regulation (EU) 910/2014.

7.2 Changes in terminology

Some changes in the terminology occurred between the eSignature Directive and the eIDAS Regulation. A general terminology change is that 'signature-verification data' changed to 'signature validation data'.[45]

Furthermore, while the Directive defined Certification-Service-Provider (CSP) as the entity or legal or natural person who issues certificates or provides other services related to electronic signatures, the Regulation does not use this term anymore but uses the broader term Trust Service Provider.[46] A Trust Service Provider (TSP) is a natural or legal person who provides one or more trust services either as a qualified or as a non-qualified TSP. A trust service is an electronic service, normally provided for remuneration, which consists of:

(a) The creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to these services; or
(b) The creation, verification and validation for website authentication; or
(c) The preservation of electronic signatures, seals or certificates relating to those services;[47]

In the eIDAS Regulation the definition of electronic signature reads as 'data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign', which is very similar to the definition in the eSignature Directive. However, the Directive still stated that electronic signatures serve as a method of authentication, while the Regulation clarifies that from the two possible functions, the function of the electronic signature is the signing function.[48]

7.3 Advanced electronic signature

The 'advanced electronic signature' in the Regulation is in the definition close to the one in the Directive, being an electronic signature which meets the following requirements:

[45] See definition of certificate in both legislative texts.
[46] A. Roßnagel, "Der Anwendungsbereich der eIDAS-Verordnung – Welche Regelungen des deutschen Rechts sind weiterhin für elektronische Signaturen anwendbar?", MMR, 2015, 359, p. 362.
[47] Art. 3 (16) Regulation (EU) 910/2014.
[48] Art. 3 (10) Regulation (EU) 910/2014.

Advanced electronic signature:

- Uniquely linked to the signatory;
- Is capable of identifying the signatory;
- Is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and
- Is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

Comparing the requirements of the eSignature Directive with those of the Regulation, it seems that the requirements of the Regulation are slightly less strict. The Directive had still required a creation with means that the signatory can maintain under his sole control, while the Regulation only requires a high level of confidence.[49] The Commission shall define reference formats of advanced electronic signatures or reference methods in case of alternative formats in implementing acts until 18th of September 2015.[50] If a signature meets the standards, which are referenced by the Commission, it can be assumed that the signature fulfils the requirements of an advanced electronic signature.[51]

7.4 Qualified electronic signature

While the eSignature Directive did not use the term 'qualified electronic signature' as such, the Regulation does use this term to refer to an advanced electronic signature (see 7.3) that is created using a qualified electronic signature creation device (see 7.5), and which is based on a qualified certificate for electronic signatures (see 7.6).[52]

[49] A. Roßnagel, "Neue Regeln für sichere elektronische Transaktionen: Die EU-Verordnung über elektronische Identifizierung und Vertrauensdienste, NJW 2014, 3686", p. 3689, and C. Seegebarth, Perspektiven aus der eIDAS-Verordnung, DuD, 10, 2014, p. 677.
[50] Art. 27 (5) Regulation (EU) 910/2014.
[51] Art. 27 (4) Regulation (EU) 910/2014.
[52] Art. 3 (12) Regulation (EU) 910/2014.

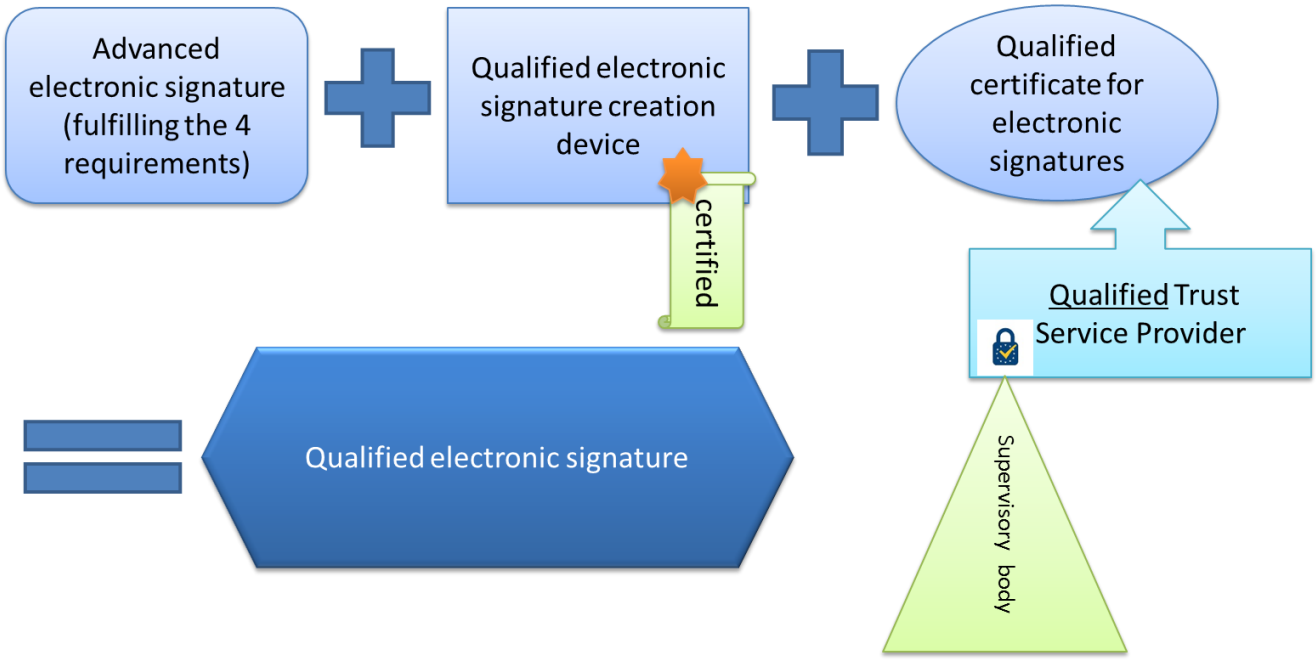

Figure 1 Requirements qualified electronic signature

7.5 Qualified electronic signature creation device

For a qualified electronic signature a 'qualified electronic signature creation device' (QESCD) is needed.

What is a QESCD?

An electronic signature creation device is software or hardware used to create an electronic signature. A qualified electronic signature creation device is basically what a secure-signature-creation device was under the eSignature Directive, albeit that the requirements of the Regulation differ slightly.[53]

In order to be qualified, the electronic signature creation devices must ensure, with regard to the electronic signature creation data, (1) that the confidentiality of it is reasonably assured, (2) that the creation data can practically occur only once, (3) that the creation data with reasonably assurance cannot be derived and (4) that the legitimate signatory can reliably protect the electronic signature creation data against use by others. In addition, it needs to ensure that the electronic signature is reliably protected against forgery by using currently available technology.

[53] See Annex II eIDAS Regulation. As a result it is also possible to use remote signing solutions, provided that it is done by a qualified TSP, which only duplicates the electronic signature creation data for back-up purposes if the security of the duplicated datasets is at the same level as for the original datasets and the number of duplicated datasets shall not exceed the minimum needed to ensure continuity of the service.

Finally, it is an important requirement that the QESCD shall not alter the data to be signed, or prevent such data from being presented to the signatory prior to signing.[54] The Commission may, by the means of implementing acts, refer to standards for QESCD.[55] If a QESCD meets these standards, it shall be presumed to be compliant to the above mentioned requirements.

To prove that the requirements are fulfilled and the device is qualified, it needs to be certified by appropriate public or private bodies designated by the Member States.[56] The Commission may adopt delegated acts outlining specific criteria that have to be met by the designated bodies, and shall establish a list of standards for the security assessment of information technology products.[57] The Member States will inform the Commission no later than one month after the certification is concluded about certified QESCD, and also notify the Commission in case the certification is cancelled and QESCD are no longer certified.[58] On the basis of this information, the Commission shall establish, publish and maintain a list of certified QESCDs.[59] The legal effect of this list is not stated in the Regulation.[60]

In recital 56 it is further specified that the Regulation does not cover the entire system environment in which a QESCD operates. Only the hardware and system software used to manage and protect the signature creation data, which has been created, stored or processed in the signature creation device, should be certified.[61] Signature creation applications are excluded from the scope of certification.[62]

7.6 Qualified certificate for electronic signatures

In order to sign with a qualified electronic signature, the signatory additionally needs a 'qualified certificate for electronic signatures'. These certificates have to be issued by a qualified TSP and must meet the requirements listed in Annex I of the eIDAS Regulation.[63] These requirements are largely similar to the requirements for qualified certificates of the eSignature Directive, with some additions. Examples are, that the certificate must now also contain the location where the

[54] Art. 29 (1) Regulation (EU) 910/2014 and Annex II.
[55] Art. 29 (2) Regulation (EU) 910/2014.
[56] Art. 30 (1) Regulation (EU) 910/2014.
[57] Art. 30 (4) and (3) Regulation (EU) 910/2014.
[58] Art. 31 (1) Regulation (EU) 910/2014; A.Roßnagel, Neue Regeln für sichere elektronische Transaktionen: Die EU-Verordnung über elektronische Identifizierung und Vertrauensdienste, NJW 2014, 3686, p. 3689.
[59] Art. 31 (2) Regulation (EU) 910/2014.
[60] A.Roßnagel, Neue Regeln für sichere elektronische Transaktionen: Die EU-Verordnung über elektronische Identifizierung und Vertrauensdienste, NJW 2014, 3686, p. 3690.
[61] Recital 56 Regulation (EU) 910/2014.
[62] Recital 56 Regulation (EU) 910/2014.
[63] A.Roßnagel, Neue Regeln für sichere elektronische Transaktionen: Die EU-Verordnung über elektronische Identifizierung und Vertrauensdienste, NJW 2014, p. 3689.

advanced electronic signature or advanced electronic seal of the issuing qualified TSP is available free of charge; or that the location of the services that can be used to enquire about the validity status of the qualified certificate must be specified in the certificate. If the creation data related to the validation data is located in a qualified electronic signature creation device, it should include an indication of this, which should be at least suitable for automated processing.[64]

Instead of requiring information on the identification of the CSP, the eIDAS Regulation requires 'a set of data unambiguously representing the QTSP' (Qualified Trust Service Provider). This includes at least the Member State in which that provider is established, for a legal person the name and possibly registration number, and for a natural person that person's name.

The Commission may establish reference numbers of standards for qualified certificates for electronic signatures. The Regulation prescribes that no other mandatory requirements shall be imposed upon qualified certificates for electronic signatures than the ones mentioned in the Regulation.[65]

It is possible that a qualified certificate will be revoked after initial activation. It will then lose its validity from the moment of its revocation, which means that signatures made before the revocation are still valid. The QTSP is obliged to register a revocation in its certificate database and publish the revocation status within 24 hours after the receipt of the request. The revocation becomes effective immediately upon its publication.[66] After being revoked, the status of the certificate shall not be reverted under any circumstances.[67]

Temporary suspension of a certificate is also possible, but would be governed by national rules.[68] The difficulty of temporary suspension is the validity of the electronic signature, since signatures created within the period of suspension may or may not be valid if the certificate is reinstated after the suspension (suspension with or without obliteration).[69] Member States may only lay down rules under the condition that the qualified certificate will lose its validity for the period of suspension and that the period of suspension will be clearly indicated in the certificate database.[70] Furthermore, the suspension status during the period of suspension should be visible from the service providing information on the status of the certificate.[71]

7.6.1 Qualified Trust Service Provider

[64] Annex I (j) Regulation (EU) 910/2014.
[65] Art. 28 (2) Regulation (EU) 910/2014.
[66] Art. 24 (3) Regulation (EU) 910/2014.
[67] Art. 28 (4) Regulation (EU) 910/2014.
[68] See C. Seegebarth, Perspektiven aus der eIDAS Verordnung, DUD 10, 2014, p. 676.
[69] See p. 10 of the study SMART 2012/0001, Phase II - Electronic signatures in public services Version 2.1, 5 June 2014.
[70] Art. 28 (5) Regulation (EU) 910/2014.
[71] Art. 28 (5) Regulation (EU) 910/2014.

In order to issue qualified certificates, the issuing TSP must be qualified.

Requirements to be qualified as a TSP

While the Directive listed the requirements for a CSP to issue a qualified certificate in Annex II, the requirements for qualified TSPs in the Regulation are listed more central within the Regulation under art. 24. The main differences to the eSignature Directive are that the requirements to verify the identity, which first only stated 'by appropriate means and in accordance with national law', are made much more explicit by including how exactly the information can be verified[72]. Furthermore, under the eIDAS Regulation the supervision has been strengthened. While under the Directive supervision was within national discretion[73] the eIDAS Regulation now provides more specific guidelines on supervision and the cooperation between different national supervisory bodies.

The Regulation further includes in the requirements for qualified TSPs that they have to inform the supervisory body of any change in the provision of their qualified trust services and an intention to cease those activities. Ceasing the activities is now explicitly referred to, and had beforehand not been considered in the Directive (though some national implementations did include it). The Directive only provided that CSPs have to demonstrate the reliability necessary for providing certification services. The eIDAS Regulation instead prescribes that a qualified TSP has to record relevant information and keep it accessible for an appropriate period of time, including after the activities of the qualified TSP have been ceased.[74] Qualified TSPs have to have an up-to-date termination plan to ensure continuity of service.[75] Finally, the importance of data protection has been made more explicit in the Regulation by stating that the qualified TSP must ensure lawful processing of personal data in accordance with the Data Protection Directive.

In order to be qualified, the TSP needs to fulfil the requirements of the Regulation, which will be confirmed via a conformity assessment report issued by a conformity assessment body.[76] The report, together with a notification of the intention to provide qualified trust services, must be

[72] These are either: by the physical presence of the natural person or of an authorised representative of the legal person; or remotely, using electronic identification means, for which prior to the issuance of the qualified certificate, a physical presence of the natural person or of an authorised representative of the legal person was ensured and which meets the requirements set out in Article 8 with regard to the assurance levels 'substantial' or 'high'; or by means of a certificate of a qualified electronic signature or of a qualified electronic seal issued after verification by physical presence; or by using other identification methods recognised at national level which provide equivalent assurance in terms of reliability to physical presence. The equivalent assurance shall be confirmed by a conformity assessment body, Art. 24 (1) Regulation (EU) 910/2014.
[73] Art. 3 (3) Directive 1999/93/EC.
[74] Art. 24 (2) h Regulation (EU) 910/2014.
[75] Art. 24 (2) i Regulation (EU) 910/2014.
[76] A. Roßnagel, Neue Regeln für sichere elektronische Transaktionen: Die EU-Verordnung über elektronische Identifizierung und Vertrauensdienste, NJW 2014, 3686", p. 3689.

submitted to the supervisory body.[77] The supervisory body verifies whether the TSP complies with the requirements, and if it does, the supervisory body will grant qualified status to the TSP and inform the national body responsible for establishing, maintaining and publishing national trusted lists.[78] After the qualified status has been indicated in the trusted list, the qualified TSP may start to provide the qualified trust services and may use the EU trust mark to indicate the qualified trust services it provides. The national trusted lists, which provide information on the qualified trust service providers, are made available in an electronically signed or sealed form suitable for automated processing.[79] The Commission will make the information on this available to the public in a way suitable for automated processing.[80]

7.7 eIDAS and national eSignature legislation

With the introduction of the eIDAS Regulation the national legislations are not invalidated, but the Regulation enjoys primacy in application, meaning that existing legislation contradictory to the Regulation will automatically be replaced by the Regulation the day of entry into force, being July 1, 2016.[81]

However, aspects that are not covered by the Regulation still can be covered by national law. For example, only trust services provided to the public having effects on third parties need to adhere to the eIDAS Regulations requirements.[82] Therefore closed services such as the German encrypted e-mail services DeMail or ePostbrief will still fall under applicable national provisions, since the eIDAS Regulation is not applicable to them.[83] Furthermore, the Regulation does not cover "*aspects related to the conclusion and validity of contracts or other legal obligations where there are requirements as regards form laid down by national or Union law. In addition, it should not affect national form requirements pertaining to public registers, in particular commercial and land registers*".[84] Therefore, for example in Germany, the provisions of the SigG and SigV are still applicable to certain signatures, such as the ones for registration in the commercial register by notaries[85] or specific provisions that are solely applicable to German public service.[86]

[77] Art. 21 (1) Regulation (EU) 910/2014.
[78] Art. 21 (2) Regulation (EU) 910/2014.
[79] Art. 22 (1) and (2) Regulation (EU) 910/2014.
[80] Art. 22 (4) Regulation (EU) 910/2014.
[81] A. Roßnagel, Neue Regeln für sichere elektronische Transaktionen: Die EU-Verordnung über elektronische Identifizierung und Vertrauensdienste, NJW 2014, 3686", p. 3691.
[82] Recital 21 Regulation (EU) 910/2014.
[83] A. Roßnagel, Neue Regeln für sichere elektronische Transaktionen: Die EU-Verordnung über elektronische Identifizierung und Vertrauensdienste, NJW 2014, 3686, p. 3687.
[84] Recital 21 Regulation (EU) 910/2014.
[85] E.g. § 12 HGB and § 39 a BeurkG.
[86] E.g. § 37 I VwVfG or § 110d SGB IV, A. Roßnagel, Neue Regeln für sichere elektronische Transaktionen: Die EU-Verordnung über elektronische Identifizierung und Vertrauensdienste, NJW 2014, 3686, p. 3691.

Also provisions which are not contradictory to provisions of the eIDAS Regulation can still be applied, in cases in which the regulation does not provide sufficient provisions or mandates implementation acts.[87]

[87] A. Roßnagel, Neue Regeln für sichere elektronische Transaktionen: Die EU-Verordnung über elektronische Identifizierung und Vertrauensdienste, NJW 2014, 3686, p. 3691.

8. The FutureID eSign service

8.1 Description FutureID eSign service

The FutureID eSign service provides a generic interface to create advanced electronic signatures. It uses a standardised request and response format, and therefore it is possible to request a signature without having to know which exact signature credential the User uses. Requesting a signature is done by sending a request to the FutureID Client. The User will then see the document that requires signing and confirms that he/she wants to sign it. Afterwards the User, with the help of the FutureID eSign service as part of the FutureID Client, can create the signature and the result will be sent back to the applicant that requested the signature.

The FutureID eSign service only supports the creation of signatures. The actual signatures will be computed/calculated on the used signature creation device (e.g. chip card) while the FutureID eSign service is responsible for the creation of the container in XAdES, CAdES or PAdES format. For validation, the request will be sent to the FutureID Client, which redirects the request to the validation service that has been selected by the User. For the current needs of the project a validation service at TUG is used, but generally any validation service can be selected by the User.

8.2 Is the eSign functionality of FutureID a trust service?

A trust service – according to the eIDAS Regulation – is an electronic service, normally provided for remuneration, which consists of, amongst others, the creation, verification, and validation of electronic signatures. Since the eSign service supports the signatory in the creation, verification and validation of the electronic signature, the question is whether this constitutes a trust service? Related to this question is also who would then be the TSP, which is considered a natural or legal person who provides one or more trust services either as a qualified or as a non-qualified TSP.[88]

First, it needs to be assessed what exactly the meaning of ‘creation’, ‘verification’ and ‘validation’ as a trust service provision of an electronic signature is. For answering this question it should be kept in mind that the provisions of the eIDAS Regulation are influenced by the technology of digital signatures, as the eSignature Directive has been beforehand (recognisable from the fact

[88] Art. 3 (19) Regulation (EU) 910/2014.

that for a qualified electronic signature a qualified certificate is required, which is characteristic of PKI technology).[89] Therefore, 'creation, verification and validation' should be viewed in this light.

'Creation' in the context of trust services should therefore in this case not be understood as the factual creation of the signature by the signatory. 'Creation' of electronic signatures as an electronic service most likely means providing the service of remote creation of electronic signatures.[90]

Signature verification and validation are closely connected, as can be seen in art. 3 (41) eIDAS Regulation where validation is defined as "the process of verifying and confirming that an electronic signature (…) is valid". The standard ETSI TS 102 853 defines signature verification as a process of checking the cryptographic value of a signature using signature verification data, while signature validation is defined as the process of checking that a signature is valid including overall checks of the signature against local or shared signature policy requirements as well as certificate validation and signature verification.[91]

The terms are so closely connected that it seems that they are sometimes used interchangeably, as can be seen by the fact that the eSignature Directive used the term 'signature-verification data' while the eIDAS Regulation uses 'signature validation data' as term for public keys.[92] The eIDAS Regulation provides that the validation is done with validation data.[93] This validation data is linked via an electronic attestation ('certificate for electronic signature') to a natural person, and the certificate confirms at least the name or the pseudonym of that person.[94]

Validation can also be provided as a service. In the IAS study referred to Signature Validation Service Providers, which means TSPs offering services in relation to electronic signatures

[89] A. Barofsky, The European Commission's Directive on electronic signatures: Technological "Favoritism" towards digital signatures, 24 B.C. Int'l & Comp. L. Rev. 145, 2000, p. 157.
[90] See, e.g., in the European Commission Feasibility study on an electronic identification, authentication and signature policy (IAS), Final Report, Luxembourg, Publications Office of the European Union, 2013, p. 17 the reference to Signature generation service provider as a TSP which provides trust services that allow secure remote management of a signatory's signature creation device and generation of electronic signatures by means of such a remotely managed device. In the same report on p.31 is referred to Signature Generation SP and Signature Validation SP as TSPs used in the signature creation or validation process.
[91] This division is also described in the European Commission, Feasibility study on an electronic identification, authentication and signature policy (IAS), Final Report, Luxembourg, Publications Office of the European Union, 2013, p. 31.
[92] See the definition of certificate in both legislative texts, and, e.g., the European Commission, Feasibility study on an electronic identification, authentication and signature policy (IAS), Final Report, Luxembourg, Publications Office of the European Union, 2013, p. 28. Private keys are referred to as Signature Creation data.
[93] Art. 3 (40) Regulation (EU) 910/2014.
[94] Art. 3 (14) Regulation (EU) 910/2014.

regarding the validation of the certificates (including the certificate chain) and the validity of the electronic signature itself.[95]

The Regulation does not refer to Signature Validation Service Providers, however, for the validation of qualified electronic signatures, it refers to specific services regarding the validation: "*specifying the requirements for qualified trust service providers that can provide a qualified validation service to relying parties unwilling or unable to carry out the validation of qualified electronic signatures themselves, should stimulate the private and public sector to invest in such services. Both elements should make qualified electronic signature validation easy and convenient for all parties at Union level*."[96]

Since the eSign service only provides the framework to easily use the service provided by other TSPs, but does not provide the creation or validation of an electronic signature as a service itself, it can be concluded that the eSign service does not constitute a trust service. The credentials to create the electronic signature will be provided by a (qualified or non-qualified) TSP. The eSign service also does not do the validation, but only shows the result of the validation. The TSPs are the natural or legal persons who provide these services, while the FutureID Client is neither a natural nor legal person and, therefore, cannot qualify as a TSP.

The validation service that is used would provide the validation as an electronic service and, therefore, constitutes a TSP.

8.3 PAdES, XAdES and CAdES still advanced electronic signatures?

Digital signatures created in accordance with the PAdES, XAdES and CAdES ETSI standards[97] are advanced electronic signatures in the meaning of the eSignature Directive. The requirements for an advanced electronic signature in the eIDAS Regulation stayed the same as in the Directive, with one exception. The requirement that the signatory must maintain the creation means under his sole control has changed and eased into the requirement that the signatory, with a high level of confidence, can use the electronic signature creation data under his sole control. Since the requirement is therefore not higher nor significantly different than before, digital signatures in accordance with the PAdES, XAdES or CAdES standard should also be considered advanced electronic signatures under the eIDAS Regulation.

[95] European Commission, Feasibility study on an electronic identification, authentication and signature policy (IAS), Final Report, Luxembourg, Publications Office of the European Union, 2013, p. 18.
[96] Recital 57 Regulation (EU) 910/2014.
[97] ETSI TS 101 903: XML Advanced Electronic Signatures (XAdES); ETSI TS 102 778-3: PDF Advanced Electronic Signature Profiles (PAdES); ETSI TS 101 733: CMS Advanced Electronic Signatures (CAdES).

8.4 Legal requirements to create and validate qualified electronic signatures

The FutureID eSign service aims to support digital signatures in the PAdES, XAdES or CAdES format, which are advanced electronic signatures. Potentially, also qualified electronic signatures can be supported by the FutureID eSign service. The necessary elements for the creation and validation of qualified electronic signatures will be specified in the following.

8.4.1 Creation

A qualified electronic signature requires an advanced electronic signature (fulfilling the 4 requirements mentioned in 7.3), created using a qualified electronic signature creation device (see 7.5) and based on a qualified certificate for electronic signatures (see 7.6).

Therefore, the User should be in possession of a certificate for electronic signatures which has been issued by a QTSP as a qualified certificate, and a qualified electronic signature creation device. If the User holds these, it should be possible to create qualified electronic signatures with the eSign service.

8.4.2 Validation

The eIDAS Regulation states special requirements for the validation of qualified electronic signatures. According to art. 32 is it necessary for a confirmation of the validity of a qualified electronic signature, that the process for the validation provides information regarding: The certificate: that it was qualified, issued by a QTSP and valid at the time of signing. The signature validation data: that it corresponds to the data provided to the relying party. The electronic signature: that it was created by a QESCD and met all the requirements of an advanced electronic signature at the time of signing. The signed data: that the integrity has not been compromised. Finally, the unique set of data representing the signatory in the certificate needs to be correctly provided, as well as the use of a pseudonym, if used.[98]

The validation system must provide the correct result of the validation process to the relying party and must allow the relying party to detect any security relevant issues.[99] Article 33 eIDAS Regulation states that a qualified validation service for qualified electronic signatures may only be provided by a QTSP who adheres to the requirements mentioned before, and additionally allows the relying parties to receive the result in an automated manner, which is reliable, efficient and bears the advanced electronic signature or advanced electronic seal of the provider of the qualified validation service.[100]

[98] Art. 32(1) Regulation (EU) 910/2014.
[99] Art. 32 (2) Regulation (EU) 910/2014.
[100] Art. 33 (1) Regulation (EU) 910/2014.

The currently used validation service of TUG for project purposes does not provide a qualified validation service, as TUG is not a qualified TSP. However, the eSign service is built in such a way that it is always possible for the User to use the validation service of his choice, which can be a qualified validation service provided by a QTSP.

Under certain circumstances a validation service could pose a privacy problem. To validate electronic signatures it is necessary to assess whether the integrity of the signed data has been compromised. In general, the integrity is assured with digital signatures by making a hash of the electronic document, which then is encrypted with the private key of the person. For the validation the public key is used. In order to assess the integrity, the hash is compared to the document, and it can be detected whether any changes have been made to the document. However, in order to do this, the validation service needs to compare the signed document with the hash. This could prove to be problematic, in case this would reveal sensitive information, like e.g. a doctor patient relationship. There are different possible solutions. One would be to have an 'in-house' validation service at the data controller side, so that no third party exists which would get access to the information. If the validation service is provided by a third party, the controller of the personal data should conclude a contract with the validation service[101], which should include a non-disclosure agreement. Another imaginable technical solution would be to encrypt the document and then sign the encrypted document in order to ensure that the validation service will not have access to the sensitive information.

8.5 Remote (qualified) electronic signatures

Remote qualified electronic signatures, such as, e.g., the Austrian mobile signature, can be used with the FutureID eSign service. Remote qualified electronic signatures are generally signatures where the SSCD/QESCD is not in the hand of the signatory, instead it is provided by a service provider. In case of e.g. the Austrian mobile signature the SSCD is the central Hardware Security Modul (HSM). The control of the signatory is, in this case, ensured by using a secret password and a two-factor authentication based on knowledge (password) and possession (mobile phone).[102]

The eSignature Directive required for an advanced electronic signature that "it is created using means that the signatory can maintain under his sole control"[103]. Since in case of remote signatures the signatory does not maintain the signature creation device under his sole control, it

[101] To the extent that the validation services acts as a processor of the personal data. For further information regarding controller-processor relationships cf. D32.8.
[102] http://www.egiz.gv.at/files/download/studie_mobile_signatur_auf_smartphones.pdf.
[103] Art. 2, 2 (c) Directive 1999/93/EC.

was questionable whether this type of services could create advanced and qualified electronic signatures under the old directive.[104]

After consultations with stakeholders, the Commission therefore changed the text of the requirements in its draft of the eIDAS Regulation from "means that the signatory can maintain under his sole control" to "electronic signature creation data that the signatory can, with high level of confidence, use under his sole control" with the accompanying explanation that "*it should be possible to entrust qualified electronic signature creation devices to the care of a third party by the signatory, provided that appropriate mechanisms and procedures are implemented to ensure that the signatory has sole control over the use of his electronic signature creation data, and the qualified signature requirements are met by the use of the device*."[105] In the final version of the eIDAS Regulation this change has been kept in Article 26 (c) and recital 52 explains that remote electronic signature creation is believed to have multiple economic benefits. In order to ensure the same legal recognition, remote electronic TSPs "*should apply specific management and administrative security procedures and use trustworthy systems and products, including secure electronic communication channels, in order to guarantee that the electronic signature creation environment is reliable and is used under the sole control of the signatory.*"[106] The requirements for qualified electronic signatures remain the same. Therefore remote qualified electronic signatures are possible under the eIDAS Regulation. However, this change in order to make remote qualified electronic signatures possible has been criticized as lowering the security level.[107]

[104] A. Roßnagel, Fremderzeugung von qualifizierten Signaturen? - ein neues Geschäftsmodell und seine Rechtsfolgen, MMR, 2008, 22, p. 27. Roßnagel criticises that for remote signature creation often the key owner leaves the secure signature creation device with the service provider and shares with him the knowledge to activate the secret signature key, which means that the two factors which ensure the connection between the signatory and the signature are in the hands of a third person.

[105] Recital 40 Proposal eIDAS, COM(2012) 238 final.

[106] Recital 52 Regulation (EU) 910/2014. See for requirements regarding the QESCD footnote 53.

[107] See for criticism at the eIDAS Regulation: A. Roßnagel, Neue Regeln für sichere elektronische Transaktionen: Die EU-Verordnung über elektronische Identifizierung und Vertrauensdienste, NJW 2014, 3686: p. 3690.

9. Conclusion

The objective of this deliverable was to provide a comprehensive analysis of the legal framework surrounding the provisioning of FutureID eSign services. In doing that, it first provided an overview of the subject of electronic signatures, delineating the difference between digital and electronic signatures. Electronic signatures are a legal concept, established European wide by the eSignature Directive and influenced by the technology of digital signatures, but at the same time intentionally technologically neutral formulated. Furthermore the development of electronic signature legislation was described, which also included an overview of German and Belgian signature law. The eSignature Directive ensured a certain harmonization with regard to the national law, however, even within these harmonized laws there was still enough difference to provide a barrier to an internal market of electronic signatures.

On the 17th of September 2014 the eIDAS Regulation entered into force. The rules for trust services will apply from 1st of July 2016, which is also the date on which the eSignature Directive will be repealed. Being a Regulation, the provisions of the eIDAS Regulation are directly applicable and do not need to be implemented in national law. In order to provide an overview, the provisions of the eIDAS Regulation regarding electronic signatures were compared with the provisions of the eSignature Directive.

By giving an overview of the provisions on electronic signatures, the legal requirements for electronic signatures have been described. In this regard the difference between advanced and qualified electronic signatures is important. Advanced electronic signatures are electronic signatures which are uniquely linked to the signatory, capable of identifying the signatory, created with a private key that the signatory can, with a high level of confidence, use under his sole control, and is linked to the signed data in such a way that any change in the data is detectable. This already provides a certain reliability regarding the legal effect of the signature, however, in order to be considered equal to a handwritten signature (with respect to its legal effect), the electronic signature needs to be qualified. Qualified electronic signatures have stricter and more extensive requirements. The focus of the FutureID eSign service is on (just) advanced electronic signatures, however, in the scope of this analysis it has also been assessed what the requirements are and whether it is possible to use the FutureID eSign service also for qualified electronic signatures. The result is positive, since the FutureID eSign service provides a generic interface for electronic signatures, which can be used with different certificates and electronic signature creation devices. Therefore, by using the required qualified certificate for electronic signatures and generating the signature with a qualified electronic signature creation device, it is also possible to create qualified electronic signatures. These can be verified by using a qualified electronic signature verification service. Furthermore, it could be established that the FutureID eSign service will not fall under the TSP provisions of the eIDAS Regulation as it does not constitute a trust service. Additionally, it has been assessed whether the change of requirements for advanced electronic signatures from Directive 1999/93/EC to the eIDAS

Regulation results in a change for the main formats supported by the eSign service, PAdES, XAdES and CAdES. In light of the fact that the eIDAS Regulation did not increase the requirements for advanced electronic signatures, the PAdES, XAdES and CAdES standards can still provide advanced electronic signatures. Finally it has been assessed whether signing with the FutureID eSign service using remote (qualified) electronic signature solutions will result in a legally accepted signature. This would not necessarily have been the case under the eSignature Directive. However, under the new eIDAS Regulation the creation of remote electronic signatures is possible, as the requirements for advanced electronic signatures have been lowered.